

Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

Jimmy Graham

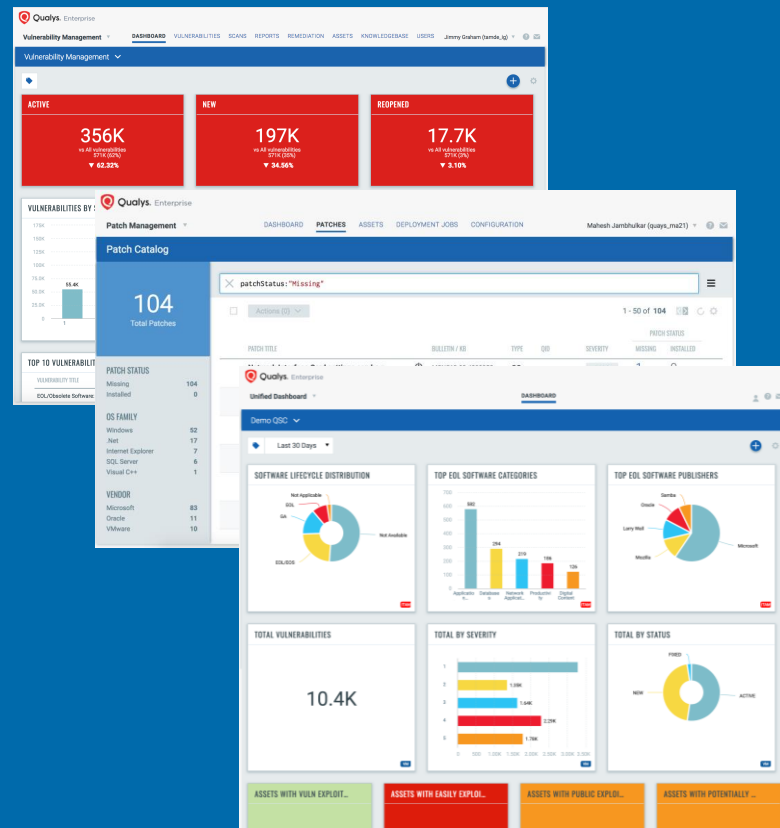
Senior Director, Product Management, Qualys, Inc.

Agenda

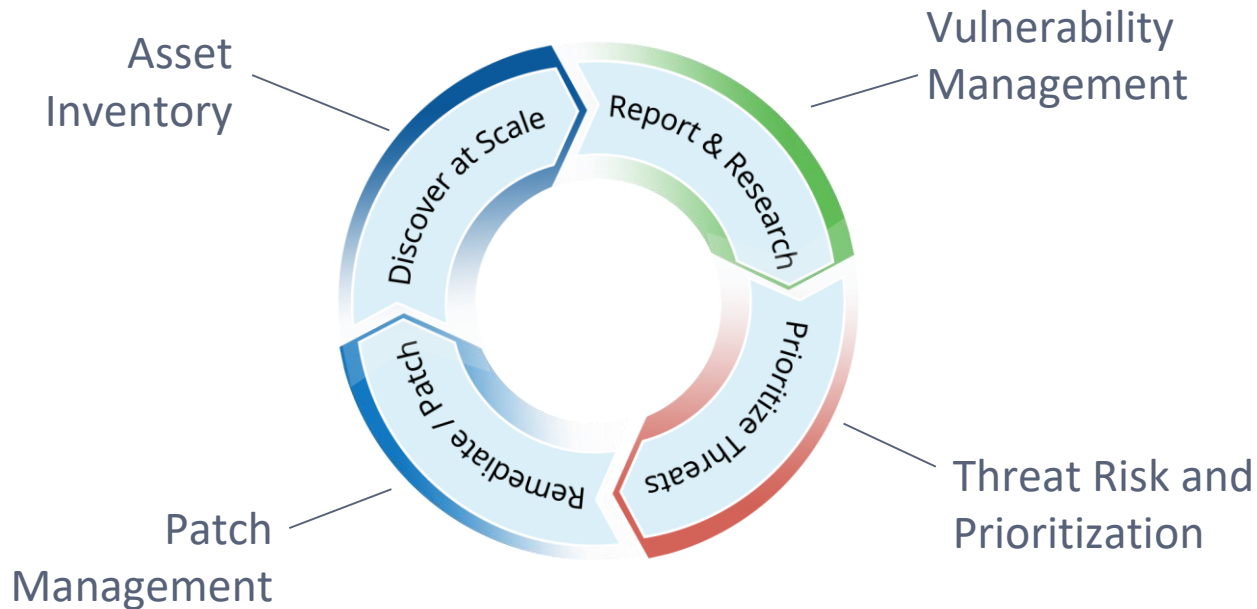
Expanding Vulnerability Management

Vulnerability Management Platform Evolution

Introducing Qualys Patch Management



Vulnerability Management Lifecycle



Expanding Vulnerability Management



Case Study: Large Bank

Challenge

Difficult to prioritize vulnerabilities across 100,000 endpoints

Manual correlation of external threat data

No active alerting on high-threat vulnerabilities

Low visibility into workstations

Solution

Threat Protection RTIs automates prioritization

Threat Protection Live Feed provides one-click access to impacted assets

Continuous Monitoring combined with RTIs

Qualys Cloud Agent for continuous and complete visibility

Vulnerability Management

Platform Evolution



Vulnerability Management ▾

DASHBOARD

VULNERABILITIES

SCANS

REPORTS

REMEDIATION

ASSETS

KNOWLEDGEBASE

USERS

Jimmy Graham (tamde_ig) ▾



Vulnerability Management ▾



ACTIVE

356K

vs All vulnerabilities
571K (62%)

▼ 62.32%

NEW

197K

vs All vulnerabilities
571K (35%)

▼ 34.56%

REOPENED

17.7K

vs All vulnerabilities
571K (3%)

▼ 3.10%

VULNERABILITIES BY SEVERITY

175K

Qualys Security Conference 2019

150K

April 29, 2019

142K

VULNERABILITIES BY TYPE

Confirmed: 318659

Potential: 255095

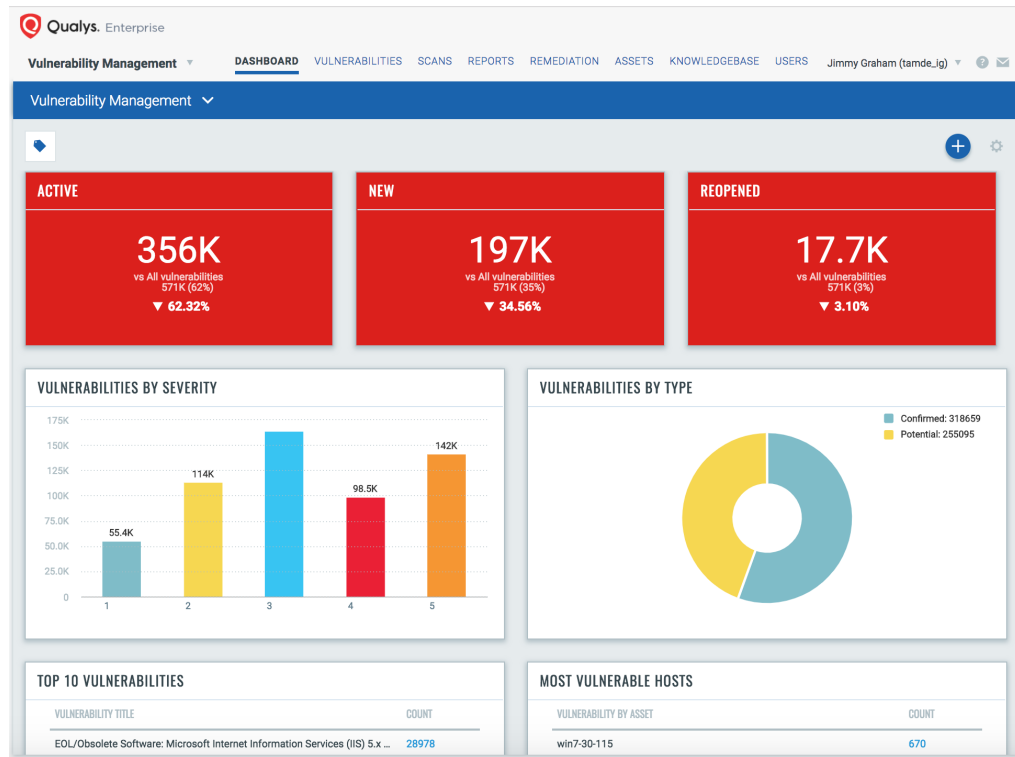
Dynamic VM Dashboard

Merges AssetView
technology into Qualys VM

Build widgets with
vulnerability counts

Search filters for quickly
building queries

Replace long-running reports
with live widgets



Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection Interface (QRDI)

Create your own or share on Qualys Community

Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic

```
{ } IPcam_QRDI.json •
1  {
2    "detection_type": "http dialog", "api_version": 1, "trigger_type": "
3    "dialog": [
4      {
5        "transaction": "http get",
6        "object": "/cgi-bin/CGIPProxy.fcgi?usr=visitor&pwd=testingqr
7        "on_error": "stop"
8      },
9      {
10       "transaction": "process",
11       "mode": "regexp",
12       "match": "<firmwareVer>(.*?)</firmwareVer>",
13       "extract": [{"var": "wholeMatch"}, {"var": "firmwareVersion"}
14     ],
15     {
16       "transaction": "report", "result": {"concat": ["Foscam Firm
17     }
18   ]
19 }
20
```




DEMO

Vulnerability Management

Dynamic Dashboard

Qualys Patch Management

Overview



Patch Management ▾

DASHBOARD

PATCHES

ASSETS

JOBS

CONFIGURATION



Patch Management ▾



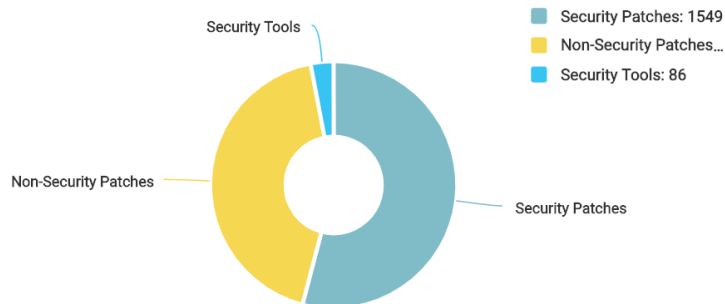
MISSING SECURITY PATCHES

1.55K

vs All Missing Patches
2.86K (54%)

▼ 54.08%

MISSING PATCHES BY CATEGORY



MISSING PATCHES

2.86K

vs All Detected Patches
3.97K (72%)

▼ 72.15%

Current Patch Management Tools

Challenges and Impact



Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation

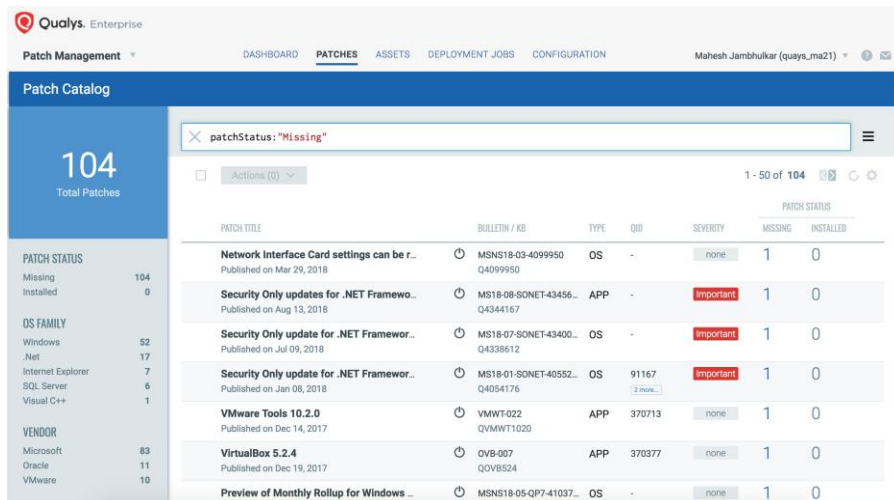
Waiting for vulnerability reports to confirm remediation

Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

Introducing Qualys Patch Management



The screenshot displays the Qualys Enterprise Patch Management interface. The top navigation bar includes 'Patch Management', 'DASHBOARD', 'PATCHES', 'ASSETS', 'DEPLOYMENT JOBS', and 'CONFIGURATION'. The user 'Mahesh Jambhulkar (qualys_ma21)' is logged in. The main section is titled 'Patch Catalog' and shows '104 Total Patches'. A search bar contains 'patchStatus:Missing'. A table lists patches with columns for Patch Title, Bulletin / KB, Type, QID, Severity, and Patch Status (Missing/Installed). The table shows several missing patches, including updates for .NET Framework, VMware Tools, and VirtualBox. A sidebar on the left provides a breakdown of patches by OS Family and Vendor.

PATCH STATUS	
Missing	Installed
104	0

PATCH STATUS	PATCH TITLE	BULLETIN / KB	TYPE	QID	SEVERITY	MISSING	INSTALLED
Missing	Network Interface Card settings can be r...	MSNS18-03-4099950 Q4099950	OS	-	none	1	0
	Security Only updates for .NET Framewo...	MS18-08-SONET-43456... Q4344167	APP	-	Important	1	0
	Security Only update for .NET Framewor...	MS18-07-SONET-43400... Q4338612	OS	-	Important	1	0
	Security Only update for .NET Framewor...	MS18-01-SONET-40552... Q4054176	OS	91167	Important	1	0
	VMware Tools 10.2.0	VMWT-022 QVMWT1020	APP	370713	none	1	0
	VirtualBox 5.2.4	OVB-007 QOVBS24	APP	370377	none	1	0
	Preview of Monthly Rollup for Windows ...	MSNS18-05-QP7-41037...	OS	-	none	1	0

OS FAMILY	Count
Windows	52
.Net	17
Internet Explorer	7
SQL Server	6
Visual C++	1

VENDOR	Count
Microsoft	83
Oracle	11
VMware	10

Automated correlation of
vulnerability and patch data
– Which patch fixes the CVE?

Simple dashboarding for
tracking missing patches

Patch using the Qualys
Cloud Agent, anywhere

Patch OS and third-party
applications

Single solution for Windows,
macOS, and Linux

Shift From Reaction Mode to Operational Security



Always up-to-date on
missing patches

Security and IT teams can “speak the same language”

Collaboration – key to successful digital transformation

Unify discovery, prioritization, and remediation into one platform

Rapid remediation of high-profile vulnerabilities in days vs. weeks

Regularly scheduled deployments are repeatable and reported on



DEMO

Patch Management

Platform Support



XP SP3+

Vista

Windows 7

Windows 8/8.1

Windows 10

Server 2003 SP2+

Server 2008/R2

Server 2012/R2

Server 2016

Server 2019



OS X 10.10
Yosemite

OS X 10.11
El Capitan

macOS 10.12
Sierra

macOS 10.13
High Sierra

macOS 10.14
Mojave



RHEL 6,7

CentOS 5.4+,6,7

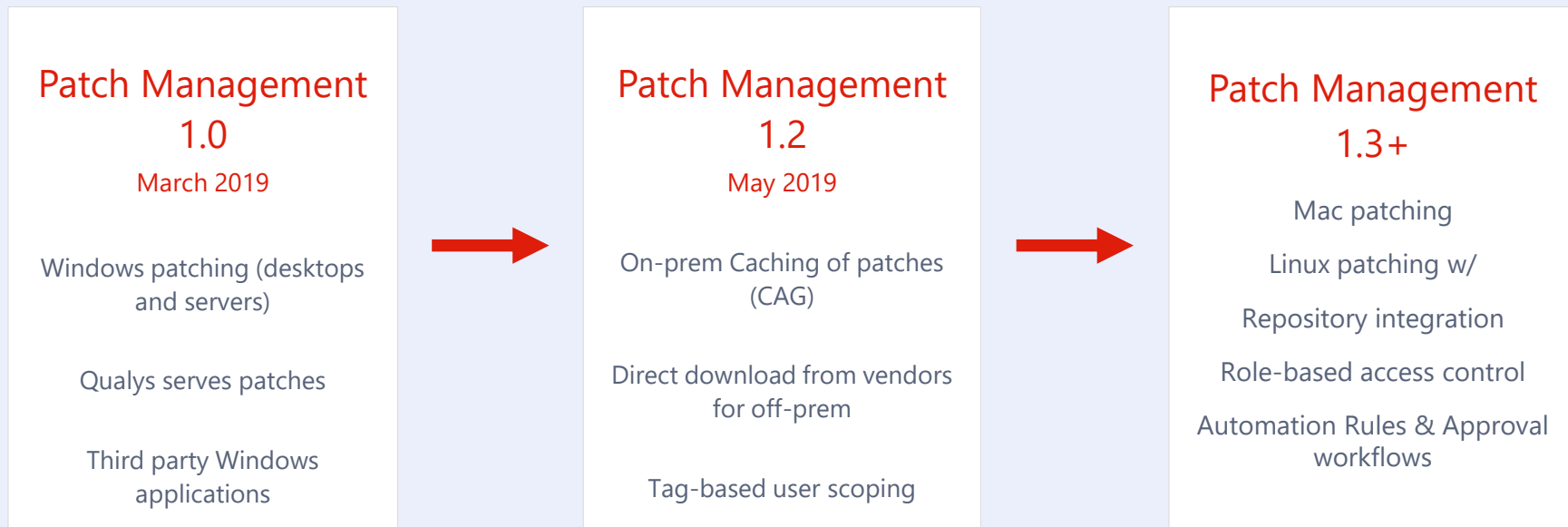
SUSE Linux Enterprise
Server/ Desktop
11,12,15

Oracle Ent Linux
6,7(Server)

Ubuntu
14.x,15.x,16.x,18.x

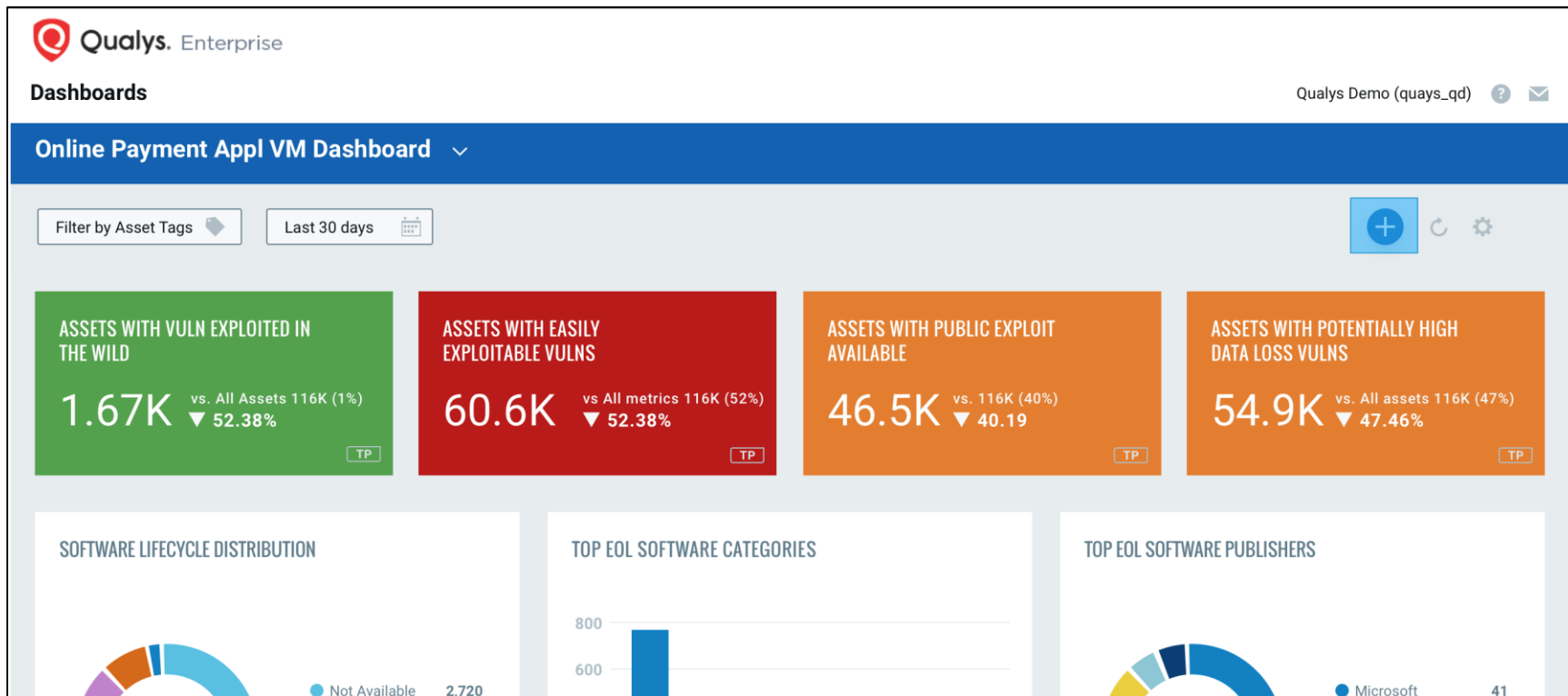
* Roadmap items are future-looking; timing and specifications may change

Patch Management Roadmap



Qualys Unified Dashboard

Preview



Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags





PREVIEW

Unified Dashboard

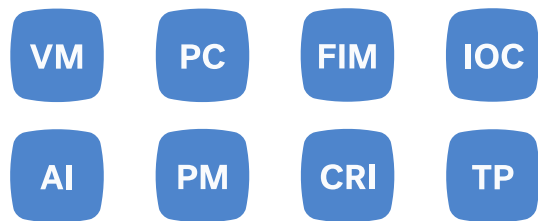
Unified Dashboard Rollout

Phase 1 – Q3 2019

Unified Dashboard App

Global dashboard filters

Support for:



Phase 2 – Q1 2020

Unified widget builder

Upgrade existing Cloud App
Dashboards

Support for:



Thank You

Jimmy Graham

jgraham@qualys.com